Method for preventing unauthorised deviations from an application development protocol in a data exchange system.

Publication number: EP0466969
Publication date: 1992-01-22
Inventor: HUESKE THOMAS DIPL-MATH (DE); JOST HILDEGARD DIPL-MATH (DE); MUELLER KLAUS DIPL-MATH (DE); PFAU AXEL DIPL-MATH (DE)
Applicant: SIEMENS NIXDORF INF SYST (DE)
Classification:
- international: ***G07F7/10;*** **G07F7/10**; (IPC1-7): G07F7/10
- European: G07F7/10D10M
Application number: EP19900113990 19900720
Priority number(s): EP19900113990 19900720

Also published as:
US5293577 (A1)
EP0466969 (B1)

Cited documents:
DE3736190
EP0190733
WO8707062
EP0159651

Report a data error here

Abstract of **EP0466969**

A data exchange system comprises for example a terminal T and a chip card K. For different applications (e.g. cash dispensing machine, computer access) basic functions B stored in the chip card K are processed in each case in a sequence specified in a protocol. Since the basic functions B can be called up from the terminal T, data security could be jeopardised through specific modifications to the protocol development at the terminal T. By storing the permissible protocols in a control list STL and by setting up a status memory area ZS on the chip card K, it is possible to monitor the protocol development on the chip card K independently from the terminal T. The relevant status Z of an application is fixed in the status memory area ZS. All basic function designations Bn which are permissible for a status Z are stored in the control list STL.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer: **0 466 969 A1**

(12) EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: **90113990.7**

(51) Int. Cl.5: **G07F 7/10**

(22) Anmeldetag: **20.07.90**

(43) Veröffentlichungstag der Anmeldung:
22.01.92 Patentblatt 92/04

(84) Benannte Vertragsstaaten:
AT BE CH DE DK ES FR GB GR IT LI LU NL SE

(71) Anmelder: **Siemens Nixdorf Informationssysteme AG**
Otto-Hahn-Ring 6
W-8000 München 83(DE)

(72) Erfinder: **Hueske, Thomas, Dipl.-Math.**
Zittelstrasse 9
W-8000 München 40(DE)

Erfinder: **Jost, Hildegard, Dipl.-Math.**
Gravelottenstrasse 1a
W-8000 München 80(DE)
Erfinder: **Müller, Klaus, Dipl.-Math.**
Nauplia Allee 14
W-8012 Ottobrunn(DE)
Erfinder: **Pfau, Axel, Dipl.-Math.**
Gabelsberger Strasse 48f
W-8000 München 2(DE)

(74) Vertreter: **Fuchs, Franz-Josef, Dr.-Ing. et al**
Postfach 22 13 17
W-8000 München 22(DE)

(54) Verfahren zur Verhinderung unzulässiger Abweichungen vom Ablaufprotokoll einer Anwendung bei einem Datenaustauschsystem.

(57) Ein Datenaustauschsystem umfaßt beispielsweise ein Terminal T und eine Chipkarte K. Für verschiedene Anwendungen (z.B. Geldautomat, Rechnerzugang) werden in der Chipkarte K gespeicherte Basisfunktionen B in einer jeweils in einem Protokoll festgelegten Reihenfolge abgearbeitet. Da die Basisfunktionen B vom Termial T aus aufgerufen werden, könnte durch gezielte Änderungen des Protokollablaufes am Terminal T die Datensicherheit beeinträchtigt werden. Durch Speichern der zulässigen Protokolle in einer Steuerliste STL und Einrichten eines Zustandsspeicherbereiches ZS auf der Chipkarte K wird es möglich, den Protokollablauf auf der Chipkarte K unabhängig vom Terminal T zu kontrollieren. Der jeweilige Zustand Z einer Anwendung wird im Zustandsspeicherbereich ZS fixiert. In der Steuerliste STL sind sämtliche bei einem Zustand Z zulässigen Basisfunktionsbezeichnungen Bn abgelegt.

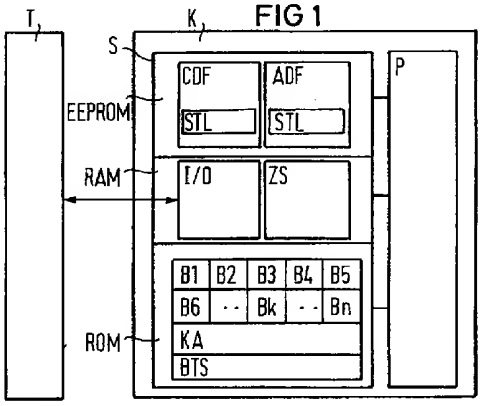


FIG 1

EP 0 466 969 A1

Tragbare Datenträger sind magnetische, optische oder sonstige physikalische Speichereigenschaften nutzende Objekte. Wenn diesen Datenträgern Intelligenz in Form eines Mikroprozessors zugeordnet ist, sind diese Datenträger besonders vielseitig verwendbar und erfüllen höchste Anforderungen an die Datensicherheit. Am meisten verbreitet sind diese intelligenten Datenträger in Form von Chipkarten.

Die Chipkarte ist vielseitig anwendbar, beispielsweise als bargeldloses Zahlungsmittel, als Personal- oder Versicherungsausweis, als Schlüssel zum Zugang zu Rechnern und für alle sonstigen Anwendungen, bei denen die eindeutige Identifizierung eines Anwenders notwendig ist oder die Berechtigung eines Anwenders eine bestimmte Anwendung auszuführen, nachgewiesen werden muß. Ist eine einzige Chipkarte für mehrere solche Anwendungen verwendbar, so spricht man von einer multifunktionalen Chipkarte. Auf Grund ihres physikalischen Aufbaus - neben dem Prozessor sind auf dem Chip ein maskenprogrammierbarer ROM-Speicherbereich, ein als Arbeitsspeicher dienender schneller RAM-Speicherbereich und ein nicht flüchtiger, programmierbarer Speicherbereich (EEPROM-Speicherbereich) untergebracht - können die Chipkarten vom Kartenherausgeber durch entsprechende Programmierung des EEPROM-Speicherbereichs für viele Anwendungen programmiert werden. Bei jeder Anwendung müssen gemäß einem vorgegebenen Protokoll einige der im ROM-Speicherbereich abgelegten Basisfunktionen auf der Chipkarte abgearbeitet werden.

Für jede Anwendung ist im EEPROM-Speicherbereich ein Anwendungsdatenfeld eingerichtet. Auf in einem solchen Feld eingetragene Daten kann eine Basisfunktion nur zugreifen, wenn diese Anwendung vorher aufgerufen wurde. Im Anwendungsdatenfeld können Daten mit unterschiedlichen Zugriffsbedingungen abgelegt sein. Es kann beispielsweise festgelegt sein, daß Daten nur dann gelesen oder verändert werden können, wenn sich der Chipkartenbenutzer durch eine PIN-Nummer (persönliche Identifikationsnummer) zu erkennen gibt.

Die Informationen, welche Anwendung vorliegt, welche Basisfunktion abgearbeitet werden soll, und die zur Berechtigungsprüfung erforderlichen Informationen erhält die Chipkarte durch Datenaustausch mit einem Terminal. Mit diesem Terminal ist die Chipkarte direkt durch elektrische Kontakte oder indirekt über optische oder induktive Koppeleinrichtungen verbunden. Vom Terminal aus können also Basisfunktionen zur Abarbeitung auf der Chipkarte aufgerufen werden. Die Reihenfolge, in der diese Basisfunktionen aufgerufen werden, wird demnach vom Terminal bestimmt. Da es aus sicherheitstechnischen Gründen erforderlich ist, die Basisfunktionen in einer bestimmten Reihenfolge abzuarbeiten, besteht durch eine mögliche Manipulation am Terminal, durch die die Ablaufreihenfolge verändert werden könnte, oder durch die bestimmte Basisfunktionen ausgelassen werden könnten, ein Sicherheitsrisiko.

Der Erfindung liegt die Aufgabe zugrunde, bei einem Datenaustauschsystem der eingangs genannten Art das sicherheitstechnische Risiko der unzulässigen, durch Manipulation am Terminal herbeigeführten Veränderung eines Ablaufprotokolls einer Anwendung auszuschalten.

Diese Aufgabe wird erfindungsgemäß durch die im Patentanspruch 1 angegebenen Merkmale gelöst.

Durch die Speicherung der zulässigen Protokollabläufe auf dem Datenträger selbst und der erfindungsgemäßen Nutzung dieser Speicherung im Zusammenwirken mit dem Zustandsspeicherbereich, wird die Sicherheit des Datenaustauschsystems zusätzlich erhöht. Der Datenträger selbst kann Manipulationen am Terminal erkennen und geeignete Gegenmaßnahmen einleiten. Zudem kann das erfindungsgemäße Verfahren für beliebige Anwendungen eingesetzt werden.

Besondere Ausgestaltungen und Weiterbildungen des erfindungsgemäßen Verfahrens und einer Vorrichtung zur Durchführung des Verfahrens sind in den Unteransprüchen angegeben.

Im folgenden wird ein Ausführungsbeispiel der Erfindung anhand der Zeichnungen näher erläutert. Dabei zeigen

FIG 1 eine Datenaustauschvorrichtung zur Durchführung des erfindungsgemäßen Verfahrens,

FIG 2 ein Ablaufdiagramm einer Anwendung,

FIG 3 eine Nachfolgertabelle zum Ablaufdiagramm,

FIG 4 Auszüge aus einer Steuerliste zum Ablaufdiagramm und

FIG 5 einen Zustandsspeicherbereich des Datenträgers.

FIG 1 zeigt ein Datenaustauschsystem, bestehend aus einem vorzugsweise als Chipkarte K ausgebildeten Datenträger und einem Terminal T. Das Terminal T ist ein mit einer Schnittstelle zum Datenaustausch mit einer Chipkarte K ausgestattetes Datenein-/ausgabegrät einer Datenverarbeitungsanlage, beispielsweise ein Geldautomat, ein Kontoauszugdrucker, eine Personenidentifizierungseinrichtung oder auch ein entsprechend ausgerüsteter Telefonapparat.

Anstelle einer Chipkarte K sind auch andere Datenträger denkbar, die von der geometrischen Form der Chipkarte K mehr oder weniger abweichen. Maßgeblich ist lediglich, daß der Datenträger einen Prozessor P und einen Speicher S enthält. Im Ausführungsbeispiel sind die Chipkarte K und

das Terminal T über elektrische Kontakte lösbar miteinander verbunden.

Der Speicher S der Chipkarte K ist in drei sich in der Speichertechnik unterscheidende Bereiche eingeteilt: Ein elektrisch lösch- und wiederbeschreibbarer Speicherteil EEPROM, ein schneller, als Arbeitsspeicher benutzter schreib- und lesbarer Speicher RAM und ein maskenprogrammierbarer Speicherbereich ROM. Gemäß ihrer Speichereigenschaften werden die drei Speicherbereiche unterschiedlich genutzt. Im maskenprogrammierbaren Speicherbereich ROM sind vom Kartenhersteller die anwenderunabhängigen, universell anwendbaren Daten und Programme gespeichert. Unter anderem sind in diesem maskenprogrammierbaren Speicherbereich ROM mehrere Basisfunktionen B mit den Basisfunktionsbezeichnungen B1...Bn, Krypto-Algorithmen KA beispielsweise zur Verschlüsselung der Daten beim Datenaustausch und ein Betriebssystem BTS der Chipkarte K eingetragen. Im schreib- und lesbaren Speicherbereich RAM werden solche Daten abgelegt, die während der Dauer einer Verbindung zwischen Terminal T und Chipkarte K benötigt werden. Unter anderem sind das die Ein-/Ausgangsdaten I/O und Daten, die in einem Zustandsspeicherbereich ZS abgelegt werden. Im elektrisch schreib- und löschbaren Speicherbereich EEPROM werden die vom Kartenherausgeber festgelegten Daten gespeichert. Dieser Speicherbereich EEPROM enthält in einem sogenannten Gemeinschaftsdatenfeld CDF hinterlegte Daten, die unabhängig von einer speziellen Anwendung verwendet werden können und Daten, auf die nur bezüglich einer Anwendung zugegriffen werden kann. Diese anwendungsspezifischen Daten sind in sogenannten Anwendungsdatenfeldern ADF abgelegt. Das Gemeinschaftsdatenfeld CDF und die Andwendungsdatenfelder ADF enthalten zusätzlich sogenannte Steuerlisten STL, in denen jeweils mindestens die Ablaufreihenfolge einer Anwendung festgelegt ist. Eine einem bestimmten Anwendungsdatenfeld ADF zugeordnete Steuerliste STL kann auch außerhalb des Anwendungsdatenfeldes ADF im Gemeinschaftsdatenfeld CDF gespeichert werden. Dies ist immer dann sinnvoll, wenn für verschiedene Anwendungen die gleiche Ablaufreihenfolge vorgeschrieben ist. Da die Steuerliste STL dann für zwei oder mehrere solcher Anwendungen nur einmal gespeichert werden muß kann Speicherplatz gespart werden.

In FIG 2 ist das Ablaufdiagramm einer Anwendung dargestellt. Ausgehend von einem Anfangszustand Z1 folgt durch Abarbeitung einer vierten Basisfunktion B4 auf den Anfangszustand Z1 ein zweiter Zustand Z2. Von diesem zweiten Zustand Z2 ausgehend, ist alternativ die Abarbeitung zweier Basisfunktionen B2, B3 möglich. Mit erfolgreicher Abarbeitung der zweiten Basisfunktion B2 kommt die Anwendung in einen dritten Zustand Z3 und mit der erfolgreichen Abarbeitung der dritten Basisfunktion B3 gerät die Anwendung in einen vierten Zustand Z4. Vom vierten Zustand Z4 ausgehend ist nur die Abarbeitung der ersten Basisfunktion B1 erlaubt, wodurch die Anwendung in einen fünften Zustand Z5 gerät. Von diesem fünften Zustand Z5 ausgehend, ist entweder die Abarbeitung der zweiten Basisfunktion B2 oder der dritten Basisfunktion B3 zugelassen, während die Abarbeitung der dritten Basisfunktion B3 zum vierten Zustand Z4 der Anwendung zurückführt, führt die Abarbeitung der zweiten Basisfunktion B2 zu einem Endzustand Z6 der Anwendung. Wenn, vom zweiten Zustand Z2 ausgehend, die zweite Basisfunktion B2 abgearbeitet wird, gerät die Anwendung in den dritten Zustand Z3. Von diesem Zustand Z3 ausgehend ist lediglich die Abarbeitung der fünften Basisfunktion B5 zulässig, die zum Endzustand Z6 der Anwendung führt. Zusätzlich ist bei jedem Zustand Z der Anwendung die Abarbeitung einer sechsten Basisfunktion B6 und einer schließenden Basisfunktion BC erlaubt. Stellvertretend für sämtliche sechsten Basisfunktionen B6 ist diese nur beim dritten Zustand Z3 der Anwendung in der FIG 2 eingezeichnet. Die Abarbeitung der sechsten Basisfunktion B6 führt immer wieder zu dem Zustand Z zurück, von dem sie ausging. Die Abarbeitung der schließenden Basisfunktion BC führt stets zur Beendigung der Anwendung.

In FIG 3 ist eine Nachfolgertabelle abgebildet. In der ersten Spalte sind sämtliche innerhalb der Anwendung möglichen Zustände Z mit den Nummern 1 bis 6 eingetragen. In der zweiten Spalte ist zu jedem Zustand die Anzahl BA der zulässigen Basisfunktionen B eingetragen. Gemäß dem Ablaufdiagramm aus FIG 2 sind dies zwei Basisfunktionen B zum ersten Zustand Z1, drei Basisfunktionen B zum zweiten Zustand Z2, zwei Basisfunktionen B zum dritten Zustand Z3, zwei Basisfunktionen B zum vierten Zustand Z4, drei Basisfunktionen B zum fünften Zustand Z5 und zwei Basisfunktionen B zum sechsten Zustand Z6. Da das Beenden einer Anwendung keinen Anwendungszustand zur Folge hat, ist die bei jedem Zustand Z mögliche schließende Basisfunktion BC in der Nachfolgertabelle der FIG 3 nicht berücksichtigt. Nach der zweiten Spalte sind in der Tabelle mehrere Spaltenpaare angegeben. Die Zahl der Spaltenpaare entspricht der maximalen Anzahl BA der zulässigen Basisfunktionen B, die auf einen Zustand Z folgen können. Jedes Spaltenpaar besteht aus einer Spalte, in der die Nummer B1...B6 der jeweils zulässigen Basisfunktion B angegeben ist und aus einer zweiten Spalte, in die die Folgezustandsbezeichnung ZF, des auf den jeweiligen Zustand Z nach Abarbeitung einer Basisfunktion B folgenden Zustandes Z1...Z6 eingetragen ist. So sind beispiels-

weise im zweiten Zustand Z2 drei Basisfunktionen B zur Abarbeitung zugelassen, nämlich die zweite Basisfunktion B2, die dritte Basisfunktion B3 und die sechste Basisfunktion B6. Auf die zweite Basisfunktion B2 folgt der dritte Zustand Z3, auf die dritte Basisfunktion B3 folgt der vierte Zustand Z4 und auf die sechste Basisfunktion B6 folgt der zweite Zustand Z2.

Die Nachfolgertabelle gemäß FIG 3 könnte in dieser Form zwar abgespeichert werden; diese Speicherform hätte aber einen hohen Aufwand bei der Auswertung dieser Tabelle zur Folge. Deshalb wird die Nachfolgetabelle in Form einer Steuerliste STL, wie sie in FIG 4 angegeben ist, gespeichert.

FIG 4 zeigt ausschnittsweise eine Steuerliste STL, die in zwei Speicherbereiche S1 und S2 eingetragen ist. Im Speicherbereich S1 sind ein Steuerlistenkopf SK und ein Steuerlistenrumpf SR untergebracht und im Speicherbereich 52 ist eine Ausnahmenliste SA abgelegt. Der Steuerlistenkopf SK enthält je einen Speicherplatz für eine Steuerlistenkopflänge SKL und für eine Ausnahmenlistenblocknummer SAN. Desweiteren enthält der Steuerlistenkopf SK nacheinander den zulässigen Zuständen Z in aufsteigender Reihenfolge zugeordnete Speicherplatzpaare, in die jeweils die Anzahl SBA der beim betreffenden Zustand Z zulässigen Basisfunktionen B (mit Ausnahme der Basisfunktionen B, dessen Basisfunktionsbezeichnungen Bn in einer Ausnahmenliste SA eingetragen sind) und ein Pointer SBP eingetragen sind. Dieser Pointer SBP zeigt auf einen Speicherplatz im Steuerlistenrumpf SR, an dem die zulässigen Basisfunktionen B und ihre Folgezustände ZF abgelegt sind. Der Steuerlistenrumpf SR besteht aus Gruppen von Datentupeln, wobei auf den Anfang jeder Gruppe der Pointer SBP aus dem Steuerlistenkopf SK zeigt. Ein solches Tupel setzt sich aus einem Speicherplatz für die Bezeichnung einer Basisfunktion B und einem Speicherplatz für eine Folgezustandsbezeichnung ZF eines zwingend auf die im Tupel bezeichnete Basisfunktion B folgenden Zustandes Z zusammen. Wie die FIG 4 zeigt, sind im Steuerlistenkopf SK dem ersten Zustand Z1 eine Funktionsanzahl SBA1 und ein Pointer SBP1 zugeordnet. Der Pointer SBP1 weist auf die dem ersten Zustand Z1 zugeordnete Gruppe im Steuerlistenrumpf SR, die ein Datentupel enthält. In die Speicherplätze dieses Datentupels sind die Bezeichnung der vierten Basisfunktion B4 und die Folgezustandsbezeichnung ZF des auf die erfolgreiche Abarbeitung der vierten Basisfunktion B4 folgenden zweiten Zustandes Z2 eingetragen. Diese Eintragungen entsprechen den Eintragungen, die an entsprechender Stelle aus FIG 2 bzw. FIG 3 entnehmbar sind.

Da zu allen Zuständen Z der Anwendung die Abarbeitung der sechsten Basisfunktion B6 und die Abarbeitung der die Anwendung beendenden schließenden Basisfunktion BC zulässig ist, ist es vorteilhaft, diese Basisfunktionen nicht im Steuerlistenrumpf SR einzutragen. Durch die Einrichtung der Ausnahmenliste SA im zweiten Speicherbereich S2 können die Bezeichnungen der bei jedem Zustand Z zulässigen Basisfunktionen B6, BC speicherplatzsparend in eine Steuerliste STL eingefügt werden. Im Steuerlistenkopf SK ist in den Speicherplatz neben der Steuerlistenkopflänge SKL eine Ausnahmenlistenblocknummer SAN eingetragen. Durch diese Nummer wird die Ausnahmenliste SA der Anwendung zugeordnet. Durch diese Art der Ausnahmenlistenzuordnung und gemeinsam mit der Speicherung der Ausnahmenliste SA im Gemeinschaftsdatenfeld CDF ist es auch möglich, eine Ausnahmenliste SA für verschiedene Anwendungen zu verwenden.

FIG 5 zeigt eine spezielle Ausführung des Zustandsspeicherbereiches ZS. Der Zustandsspeicher ZS enthält Informationen zum Protokollablauf und zur Datenzugriffskontrolle. Zu den Informationen zum Protokollablauf gehören die Blocknummer STB der Steuerliste STL, die Bezeichnung der zuletzt erfolgreich abgearbeiteten Basisfunktion B, die im Basisfunktionsspeicherplatz BZ eingetragen ist und die Information über den aktuellen Protokollzustand Z, die im Protokollzustandsspeicherplatz Zi abgelegt ist. Die Speicherplätze zur Datenzugriffskontrolle umfassen einen Platz APIN für die Kennzeichnung einer erfolgreich durchgeführten PIN-Prüfung innerhalb der Anwendung, zwei Speicherplätze zum Ablegen der Information, ob zwei verschiedene Authentizitätsprüfungen AUTH1, AUTH2 erfolgreich durchgeführt wurden, einige Reservespeicherplätze RES und einen Speicherplatz, in dem die Information eingetragen wird, ob eine globale PIN-Prüfung GPIN erfolgreich durchgeführt wurde.

Im folgenden wird der Ablauf des erfindungsgemäßen Verfahrens unter Einbeziehung der oben beschriebenen Vorrichtung erläutert.

Mit dem Einstecken einer Chipkarte K in das Terminal T wird mittels elektrischer Kontakte oder gegebenenfalls auch kontaktlos eine elektrische Verbindung zwischen Terminal T und Chipkarte K hergestellt. Diese Verbindung wirkt sowohl hinsichtlich der Stromversorgung als auch bezüglich der Ankopplung der Ein-/Ausgabeeinrichtungen I/O des Terminals T und der Chipkarte K. Durch das Einstecken der Chipkarte K wird der gesamte Arbeitsspeicherbereich in einen bestimmten Zustand - z.B. alle Bit = 0 - zurückgesetzt.

Das Terminal T ist in diesem Beispiel einer bestimmten Anwendung - beispielsweise einem Geldautomaten einer Bank - zugeordnet. Die jeweilige Art der Anwendung wird der Chipkarte K in der Weise mitgeteilt, daß das Terminal T ein spezifisches Applikationskommando an die Chipkarte K

überträgt. Auf der Chipkarte K wird nun überprüft, ob auf der Chipkarte K ein Anwendungsdatenfeld ADF für diese spezielle Anwendung vorhanden ist. Ist dieses Anwendungsdatenfeld ADF vorhanden, findet eine teilweise Initialisierung des Zustandsspeicherbereichs ZS statt. Diese Initialisierung hat zur Folge, daß die Blocknummer STB der dieser Anwendung zugeordneten, im Anwendungsdatenfeld ADF oder im Gemeinschaftsdatenfeld CDF vermerkten Steuerliste STL im Zustandsspeicherbereich ZS eingetragen wird und der Protokollzustandsspeicherplatz Zi, in dem der aktuelle Anwendungszustand Z eingetragen werden muß, auf den ersten Zustand Z1 gesetzt wird. Desweiteren werden sämtliche Bit der anwendungsbezogenen Speicherplätze zurückgesetzt (beispielsweise 0). Die Bit der Speicherplätze für globale Daten bleiben unverändert.

Nach der Meldung an das Terminal T, daß der Initialisierungsvorgang abgeschlossen ist, erfolgt die Übertragung eines Funktionskommandos vom Terminal T zur Chipkarte K, wobei dieses Funktionskommando, z.B. die vierte Basisfunktion B4 bezeichnet und die notwendigen Eingangsdaten für diese Basisfunktion B4 enthält. Die Chipkarte K befindet sich auf Grund der Eintragung im Zustandsspeicherbereich ZS im ersten Zustand Z1. Es wird nun im Steuerlistenkopf SK, der Steuerliste STL mit der im Zustandsspeicherbereich ZS eingetragenen Blocknummer STB, dasjenige Datenpaar gelesen, das dem ersten Zustand Z1 zugeordnet ist. Im Speicherplatz SBA1 ist eingetragen, daß in diesem ersten Zustand Z1 nur eine Basisfunktion B zulässig ist. Der neben diesem Speicherplatz eingetragene Pointer SBP1 zeigt auf die dem ersten Zustand Z1 zugeordnete Gruppe von Datentupeln. Dieses Tupel enthält die Bezeichnung der vierten Basisfunktion B4 und die Bezeichnung des auf die vierte Basisfunktion B4 folgenden Zustandes Z2. Der Vergleich der vom Terminal T übertragenen Basisfunktionsbezeichnung B4 und der Basisfunktionsbezeichnung B4, die im Datentupel des Steuerlistenrumpfes SR eingetragen ist, liefert ein positives Ergebnis. Auf Grund dieses positiven Vergleichsergebnisses wird die vierte Basisfunktion B4 unter Verwendung der mit dem Funktionskommando übertragenen Eingangsparameter abgearbeitet. Unter der Annahme, daß die vierte Basisfunktion B4, die für die PIN-Prüfung zuständige Funktion ist, und daß die PIN-Nummer vor dem Funktionsaufruf am Terminal T richtig eingegeben wurde, liefert die vierte Basisfunktion B4 das Ergebnis, daß die PIN-Prüfung erfolgreiche vorgenommen wurde. Am Basisfunktionsspeicherplatz BZ für die zuletzt erfolgreich ausgeführte Basisfunktion B des Zustandsspeicherbereiches ZS wird die Bezeichnung der vierten Basisfunktion B4 eingetragen. Zusätzlich wird an einem der Speicherplätze APIN oder GPIN, beispielsweise durch Setzen eines Bit, die erfolgreich ausgeführte PIN-Prüfung vermerkt. Welches Bit der beiden Speicherplätze gesetzt wird hängt davon ab, ob mit dem gleichen Terminal T mehrere Anwendungen realisierbar sind und davon, ob für alle Anwendungen, für die die Chipkarte K zugelassen ist, die gleiche PIN-Nummer erforderlich ist. Da im beschriebenen Fall das Terminal T ausschließlich dem Geldautomaten zugeordnet ist und damit nur eine Anwendung mit diesem Terminal T durchgeführt werden kann, wird der Speicherplatz APIN im Zustandsspeicherbereich ZS auf 1 gesetzt.

Der Zustand Z der Anwendung wird dadurch in den zweiten Zustand Z2 übergeführt, daß der im Datentupel im Steuerlistenrumpf SR neben der Basisfunktionsbezeichnung B4 in Form einer definierten Bitfolge eingetragene Zustand Z2 in den Protokollzustandsspeicherplatz Zi des Zustandsspeicherbereichs ZS eingetragen wird.

Nachdem ein Antwortsignal, das dem Terminal T die erfolgreiche Abarbeitung der vierten Basisfunktion B4 signalisiert, von der Chipkarte K zum Terminal T übertragen wurde, ist der erste Vorgang abgeschlossen. Die Chipkarte K ist wieder bereit, eine Information hier in Form eines Funktionskommandos, zu empfangen.

Das Terminal T überträgt nun ein zweites Funktionskommando zur Chipkarte K. Dieses Funktionskommando bezeichnet die dritte Basisfunktion B3 und beinhaltet die Eingangsparameter dieser Basisfunktion B3. Im Steuerlistenkopf SK wird das jeweilige Datenpaar gelesen, das dem zweiten Zustand Z2 zugeordnet ist. Im Speicherplatz SBA2, der die Anzahl der zulässigen Basisfunktionen B angibt steht die Zahl zwei. Der zugehörige Pointer SBP2 zeigt auf den ersten Speicherplatz, der dem zweiten Zustand Z2 zugeordneten Gruppe von Datentupeln im Steuerlistenrumpf SR.

Die in dieser Gruppe eingetragenen Basisfunktionsbezeichnungen B2, B3 werden mit der Basisfunktionsbezeichnung B3, die mit dem Funktionskommando zur Chipkarte K übertragen wurde, verglichen. Der Vergleich fällt positiv aus. Nach erfolgreicher Abarbeitung der dritten Basisfunktion B3 wird die Anwendung der Chipkarte K in den Zustand Z4 versetzt. Unter der Annahme, daß im Zuge der Abarbeitung der Basisfunktion B3 auf im Anwendungsdatenfeld ADF abgelegte Daten zugegriffen werden muß und dieser Zugriff nur zulässig ist, wenn vorher eine PIN-Prüfung erfolgreich durchgeführt wurde, werden vor Beginn der Abarbeitung der dritten Basisfunktion B3 die PIN-Speicherplätze APIN, GPIN im Zustandsspeicherbereich ZS gelesen. Nur wenn eines der beiden Bit auf 1 gesetzt ist, wird die dritte Basisfunktion B3 abgearbeitet. Ist diese Abarbeitung beendet, wird in den Basisfunktionsspeicherplatz BZ des Zustands-

speicherbereichs ZS die Bezeichnung der dritten Basisfunktion B3 eingetragen und im Protokollzustandsspeicherplatz Zi der vierte Zustand Z4 eingetragen. Zusätzlich wird ein Antwortsignal zum Terminal T übertragen.

Mit dem nächsten Funktionskommando wird die sechste Basisfunktion B6 angefordert und die notwendigen Eingangsparameter zur Chipkarte K übertragen. Im Steuerlistenkopf SK wird das dem vierten Zustand Z4 zugeordnete Datenpaar gelesen. Im Speicherplatz für die Funktionsanzahl SBA4 ist eine 1 eingetragen. Der Pointer SBP4 zeigt im Steuerlistenrumpf SR auf das dem vierten Zustand Z4 zugeordnete Datentupel. In diesem Datentupel steht die Basisfunktionsbezeichnung B1 der ersten Basisfunktion B und der entsprechende fünfte Folgezustand Z5. Ein Vergleich der Basisfunktionsbezeichnung B1 im Steuerlistenrumpf SR und der zur Chipkarte K übertragenen Basisfunktionsbezeichnung B6 liefert ein negatives Ergebnis. Daraufhin wird im Steuerlistenkopf SK die Ausnahmenlistenblocknummer SAN gelesen. Die in der Ausnahmenliste SA eingetragenen Basisfunktionsbezeichnungen B6, BC werden nun mit der zur Chipkarte K hin übertragenen Basisfunktionsbezeichnung B6 verglichen. Auf Grund des positiven Vergleichsergebnisses und unter der Voraussetzung, daß eventuelle Datenzugriffsbedingungen erfüllt sind, wird die sechste Basisfunktion B6 abgearbeitet. Trotz erfolgreicher Abarbeitung wird die Basisfunktionsbezeichnung B6 der sechsten Basisfunktion B nicht im Basisfunktionsspeicherplatz BZ des Zustandsspeicherbereichs ZS eingetragen. Die Eintragung im Protokollzustandsspeicherplatz Zi bleibt ebenfalls unverändert. Auch jetzt erfolgt die Übertragung eines Antwortsignals zum Terminal T.

Für den Fall, daß sich die Anwendung nach Abarbeitung der dritten Basisfunktion B3 im vierten Zustand Z4 befindet und vom Terminal T nochmals die dritte Basisfunktion B3 aufgerufen wird, liefern sämtliche Vergleiche im Steuerlistenrumpf SR und in der Ausnahmenliste SA ein negatives Ergebnis. In diesem Fall findet ein weiterer Vergleich statt. Die zur Chipkarte K übertragene Basisfunktionsbezeichnung B3 der dritten Basisfunktion B wird mit der im Zustandsspeicherbereich ZS im Basisfunktionsspeicherplatz BZ eingetragenen Basisfunktionsbezeichnung B3 verglichen. Dieser Vergleich liefert ein positives Ergebnis, wodurch die Abarbeitung der dritten Basisfunktion B3 zugelassen wird. Damit ist eine Wiederholbarkeit von Basisfunktionen B gewährleistet.

In entsprechender Weise werden die nachfolgend aufgerufenen Basisfunktionen B der Anwendungen behandelt, bis vom Terminal T die schließende Basisfunktion BC aufgerufen wird, die die Anwendung beendet. Die schließende Basisfunktion BC kann nach Abarbeitung jeder beliebigen Basisfunktion B aufgerufen werden, da die Basisfunktionsbezeichnung BC in der Ausnahmenliste SA enthalten ist. Für den Fall, daß keine Ausnahmenliste SA existiert, muß der Prozessor P für den Fall, daß sämtliche vorgenommenen Vergleiche negatives Ergebnis geliefert haben, überprüfen, ob die vom Terminal T aufgerufene Basisfunktion B die schließende Basisfunktion BC ist. Auf diese Weise kann sichergestellt werden, daß auch bei nicht vorhandener Ausnahmenliste SA die schließende Basisfunktion BC jederzeit aufrufbar ist.

Führt keine der Vergleichsmöglichkeiten zu einem positiven Ergebnis, dann wird dies dem Terminal T in Form einer selektiven Fehlermeldung mitgeteilt. Aus dieser selektiven Fehlermeldung geht beispielsweise hervor, daß der Grund für die Zurückweisung die Nichtzulässigkeit der Abarbeitung der Basisfunktion B im vorliegenden Anwendungszustand Z ist. Andere selektive Fehlermeldungen können beispielsweise anzeigen, daß die PIN-Nummer falsch eingegeben wurde oder eine PIN-Prüfung noch nicht stattgefunden hat.

In den meisten Fällen wird es genügen, mit einem Terminal T nur eine Anwendung auszuführen. In diesen Fällen genügt es, wenn erst nach Beendigung oder Abbruch einer vorher aktivierten Anwendung eine weitere Anwendung aufgerufen werden kann. Läßt man aber an einem Terminal T mehrere Anwendungen zu, dann kann es sinnvoll sein, diese Anwendungen auch ineinander verschachtelt aufzurufen. In diesen Fällen ist es dann möglich, nach der Übermittlung eines Antwortsignals von der Chipkarte K zum Terminal T, ein Applikationskommando noch vor Beendigung einer Anwendung zur Chipkarte K zu übertragen. Wenn ein Applikationskommando vor Beendigung einer Anwendung die Chipkarte K erreicht, wird der Inhalt des Zustandsspeicherbereichs ZS und eine Kennzeichnung, die die gegenwärtig laufende Anwendung eindeutig benennt, in einem Hilfsspeicher abgelegt. Dieser Hilfsspeicher kann beispielsweise im Gemeinschaftsdatenfeld CDF eingerichtet sein. Nach Sicherung dieser Daten im Hilfsspeicher wird die teilweise Initialisierung des Zustandsspeicherbereichs ZS vorgenommen. Die mit dem Applikationskommando bezeichnete eingeschobene Anwendung kann in oben beschriebener Weise bearbeitet werden. Nach Beendigung der eingeschobenen Anwendung werden die im Hilfsspeicher abgelegten Daten der unterbrochenen Anwendung wieder an ihre ursprünglichen Speicherstellen zurücktransferiert. Der Ablauf der vorher unterbrochenen Anwendung kann fortgesetzt werden.

Patentansprüche

1. Verfahren zur Verhinderung unzulässiger Abweichungen vom Ablaufprotokoll einer Anwen-

dung bei einem Datenaustauschsystem, das mindestens aus einem Terminal (T) und mindestens einem tragbaren, mindestens einen Prozessor (P) und mindestens einen Speicher (S) enthaltenden, wenigstens für eine Anwendung nutzbaren Datenträger (K) besteht, mit folgenden Merkmalen:

a) zum Datenaustausch wird der Datenträger (K) mit dem Terminal (T) verbunden, wodurch ein im Speicher (S) des Datenträgers vorhandener Zustandsspeicherbereich (ZS) in einen Grundzustand versetzt wird,

b) das Terminal (T) übermittelt an den Datenträger (K) ein Applikationskommando, das eine dem Terminal (T) zugeordnete Anwendung bezeichnet,

c) das Terminal (T) übermittelt an den Datenträger (K) ein Funktionskommando, das mindestens eine Basisfunktionsbezeichnung (Bk) einer Basisfunktion (B) enthält, die als nächste ausgeführt werden soll,

d) diese Basisfunktionsbezeichnung (Bk) wird im Datenträger (K) mit im Speicher (S) des Datenträgers (K) bezüglich der vorher bezeichneten Anwendung gespeicherten Basisfunktionsbezeichnungen (Bn) verglichen, die im vorliegenden, durch eine Eintragung im Zustandsspeicherbereich (ZS) fixierten, Protokollzustand zulässig sind,

e) nur bei positivem Vergleichsergebnis wird die der zum Datenträger (K) übermittelten Basisfunktionsbezeichnung (Bk) zugeordnete Basisfunktion (B) im Datenträger (K) ausgeführt,

f) nach erfolgreicher Basisfunktionsausführung

f1) werden die im Zustandsspeicherbereich (ZS) abgelegten Daten dem neuen Protokollzustand angepaßt,

f2) wird vom Datenträger (K) zum Terminal (T) ein Antwortsignal übertragen,

g) bis der Ablauf der Anwendung beendet ist oder abgebrochen wird, wird vom Terminal (T), nach der Übertragung eines Antwortsignals vom Datenträger (K) zum Terminal (T), durch Übermittelung eines Funktionskommandos an den Datenträger (K) die nächste auszuführende Basisfunktion (B) aufgerufen.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet,** daß durch die Übermittlung des Applikationskommandos vom Terminal (T) zum Datenträger (K) eine teilweise Initialisierung des Zustandsspeicherbereichs (ZS) ausgelöst wird.

3. Verfahren nach mindestens einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß die Übermittlung des Applikationskommandos vom Terminal (T) zum Datenträger (K) die Eintragung einer Blocknummer (STB) im Zustandsspeicherbereich (ZS) bewirkt und daß diese Blocknummer (STB) den Platz im Speicher (S) des Datenträgers (K) bezeichnet, an dem die bei der mit dem Applikationskommando bezeichneten Anwendung im jeweils vorliegenden Protokollzustand (Z) zulässigen Basisfunktionsbezeichnungen (Bn) abgelegt sind.

4. Verfahren nach mindestens einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß die Übertragung einer Information vom Terminal (T) zum Datenträger (K) nur dann erfolgen kann, wenn vorher ein Antwortsignal vom Datenträger (K) zum Terminal (T) übermittelt wurde.

5. Verfahren nach mindestens einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß durch Übermittlung eines Applikationskommandos vom Terminal (T) zum Datenträger (K) erst nach Beendigung oder Abbruch einer vorher aktivierten Anwendung eine weitere Anwendung aufgerufen werden kann.

6. Verfahren nach mindestens einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet,** daß bei Übermittlung eines Applikationskommandos vor Beendigung einer Anwendung mindestens der Inhalt des Zustandsspeicherbereichs (ZS) in einem Hilfsspeicher abgelegt wird, daß danach die teilweise Initialisierung des Zustandsspeicherbereichs (ZS) erfolgt und daß nach erfolgter Initialisierung die mit dem Applikationskommando bezeichnete eingeschobene Anwendung bearbeitet wird.

7. Verfahren nach Anspruch 6, **dadurch gekennzeichnet,** daß nach Beendigung der eingeschobenen Anwendung die im Hilfsspeicher abgelegten, der unterbrochenen Anwendung zugeordneten Daten wieder an ihre ursprünglichen Speicherstellen zurücktransferiert werden und daß der Ablauf der unterbrochenen Anwendung fortgesetzt wird.

8. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß zusätzlich zur Basisfunktionsbezeichnung (Bk) im Funktionskommando enthaltene Basisfunktionseingangsparameter an den Datenträger (K) übermittelt werden.

9. Verfahren nach mindestens einem der Ansprü-

che 3 bis 8, **dadurch gekennzeichnet,** daß nach Erhalt eines Funktionskommandos überprüft wird, ob eine Blocknummer (STB) im Zustandsspeicherbereich (ZS) eingetragen ist.

10. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß ein erster Speicherbereich (S1) des Speichers (S) daraufhin überprüft wird, ob eine Eintragung zum vorliegenden Protokollzustand (Z) der mit dem Applikationskommando bezeichneten Anwendung in diesem ersten Speicherbereich (S1) vorhanden ist.

11. Verfahren nach Anspruch 10, **dadurch gekennzeichnet,** daß im Falle einer vorhandenen Eintragung zum vorliegenden Protokollzustand (Z) die bezüglich dieses Protokollzustandes (Z) im ersten Speicherbereich (S1) gespeicherten Basisfunktionsbezeichnungen (Bn) mit der, mit dem Funktionskommando zum Datenträger (K) übermittelten Funktionsbezeichnung (Bk) verglichen werden.

12. Verfahren nach mindestens einem der Ansprüche 10 oder 11, **dadurch gekennzeichnet,** daß im Falle einer fehlenden Eintragung zum vorliegenden Protokollzustand (Z) bzw. einer Nichtübereinstimmung der übermittelten und der gespeicherten Basisfunktionsbezeichnungen (Bk,Bn) im ersten Speicherbereich (S1) in einem zweiten Speicherbereich (S2) des Speichers (S) überprüft wird, ob die zum Datenträger (K) übermittelte Basisfunktionsbezeichnung (Bk) in diesem zweiten Speicherbereich (S2) bezüglich der mit dem Applikationskommando bezeichneten Anwendung, unabhängig vom vorliegenden Protokollzustand (Z) eingetragen ist.

13. Verfahren nach mindestens einem der vorhergehenden Ansprüche 10 bis 12, **dadurch gekennzeichnet,** daß im Falle einer fehlenden Eintragung zum vorliegenden Protokollzustand Z bzw. einer Nichtübereinstimmung der übermittelten und der gespeicherten Basisfunktionsbezeichnung (Bk, Bn) sowohl im ersten Speicherbereich (S1) als auch im zweiten Speicherbereich (S2) überprüft wird, ob die übermittelte Basisfunktionsbezeichnung(Bk) die Basisfunktionsbezeichnung (BC) für die schließende Basisfunktion (B) ist.

14. Verfahren nach mindestens einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß nach erfolgreicher Ausführung einer Basisfunktion (B) die Bezeichnung dieser Basisfunktion (B) in einem Basisfunktionsspeicherplatz (BZ) des Zustandsspeicherbereichs (ZS) eingetragen wird.

15. Verfahren nach mindestens einem der Ansprüche 10 bis 14, **dadurch gekennzeichnet,** daß bei Nichtübereinstimmung der zum Datenträger (K) übermittelten Basisfunktionsbezeichnung (Bk) mit den entsprechenden Eintragungen im Speicher (S) diese übermittelte Basisfunktionsbezeichnung (Bk) mit der im Basisfunktionsspeicherplatz (BZ) des Zustandsspeicherbereichs (ZS) vermerkten Bezeichnung der zuletzt erfolgreich ausgeführten Basisfunktion (B) verglichen wird.

16. Verfahren nach mindestens einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß zu einer Basisfunktionsausführung eventuell erforderliche, im Zustandsspeicherbereich (ZS) abgelegte Zugriffsrechte auf Daten im Datenträger (K) überprüft werden.

17. Verfahren nach mindestens einem der Ansprüche 10 bis 16, **dadurch gekennzeichnet,** daß eine im ersten Speicherbereich (S1) in Verbindung mit einer gespeicherten Basisfunktionsbezeichnung (Bn) abgelegte Folgezustandsbezeichnung (ZF), nach erfolgreicher Ausführung dieser der gespeicherten Basisfunktionsbezeichnung (Bn) zugeordneten Basisfunktion (B), im Protokollzustandsspeicherplatz (Zi) des Zustandsspeicherbereichs (ZS) eingetragen wird.

18. Verfahren nach mindestens einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß nach erfolgreicher Basisfunktionsausführung zur Anpassung an den neuen Protokollzustand (Z) Informationen zum Protokollablauf und/oder zur Datenzugriffskontrolle im Zustandsspeicherbereich (ZS) eingetragen werden.

19. Verfahren nach Anspruch 18, **dadurch gekennzeichnet,** daß die Informationen zur Datenzugriffskontrolle getrennt nach anwendungsbezogenen und globalen Daten im Zustandsspeicherbereich (ZS) eingetragen werden.

20. Verfahren nach mindestens einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß bei negativem Vergleichsergebnis eine selektive Fehlermeldung vom Datenträger (K) zum Terminal (T) übermittelt wird.

21. Vorrichtung zur Durchführung des Verfahrens nach mindestens einem der Ansprüche 1 bis 20, bei der der Speicher (S) in einen gemein-

schaftliche und anwendungsbezogene Daten enthaltenden Datenspeicher (EEPROM), einen auch eine Ein-/Ausgangsschnittstelle (I/O) bedienenden Arbeitsspeicher (RAM) und einen ein Betriebssystem (BTS) und mehrere Basisfunktionen (B) enthaltenden Maskenspeicher (ROM) eingeteilt ist, **dadurch gekennzeichnet,** daß der Datenspeicher (EEPROM) für jede mögliche Anwendung eine die Zulässigen Protokollabläufe enthaltende Steuerliste (STL) enthält und daß im Arbeitsspeicher (RAM) der die jeweiligen Protokollzustände (Z) aufnehmende Zustandsspeicher (ZS) enthalten ist.

22. Vorrichtung nach Anspruch 21, **dadurch gekennzeichnet,** daß die Steuerliste (STL) in einen Steuerlistenkopf (SK) und einen Steuerlistenrumpf (SR) aufgeteilt ist.

23. Vorrichtung nach Anspruch 22, **dadurch gekennzeichnet,** daß im Steuerlistenkopf (SK) linear nacheinander die Steuerlistenkopflänge (SKL) und für jeden bei der Anwendung möglichen Zustand (Z), beginnend mit dem ersten Zustand (Z1) ein Datenpaar gespeichert ist, das aus einer die beim jeweiligen Zustand (Z) ausführbare Basisfunktionsanzahl (SBA) angebenden Information und aus einem auf eine Speicherstelle im Steuerlistenrumpf (SR) weisenden Pointer (SBP) besteht.

24. Vorrichtung nach mindestens einem der Ansprüche 22 oder 23, **dadurch gekennzeichnet,** daß der Steuerlistenrumpf (SR) wenigstens aus einer, aus jeweils mindestens einem Datentupel bestehenden, jeweils einem Zustand (Z) Zugeordneten Gruppe besteht und daß die Datentupel jeweils aus einer gespeicherten Basisfunktionsbezeichnung (Bn) und einer Folgezustandsbezeichnung (ZF) bestehen.

25. Vorrichtung nach mindestens einem der Ansprüche 23 oder 24, **dadurch gekennzeichnet,** daß der einem bestimmten Zustand (Z) zugeordnete Pointer (SBP) jeweils auf den Beginn einer dem gleichen Zustand (Z) Zugeordneten Gruppe im Steuerlistenrumpf (SR) zeigt.

26. Vorrichtung nach mindestens einem der Ansprüche 21 bis 25, **dadurch gekennzeichnet,** daß einer Steuerliste (STL) eine Ausnahmenliste (SA) zugeordnet ist.

27. Vorrichtung nach Anspruch 26, **dadurch gekennzeichnet,** daß im Steuerlistenkopf (SK) unmittelbar nach der Steuerlistenkopflänge (SKL) eine Ausnahmenlistenblocknummer (SAN) eingetragen ist, die direkt oder indirekt den Speicherplatz angibt, an dem die Ausnahmenliste (SA) gespeichert ist.

28. Vorrichtung nach mindestens einem der Ansprüche 26 oder 27, **dadurch gekennzeichnet,** daß in der Ausnahmenliste (SA) nacheinander die Basisfunktionsbezeichnungen (Bn) der Basisfunktionen (B) angegeben sind, die unabhängig vom vorliegenden Protokollzustand jederzeit ausführbar sind.

29. Vorrichtung nach mindestens einem der vorhergehenden Ansprüche 21 bis 28, **dadurch gekennzeichnet,** daß im Zustandsspeicherbereich (ZS) Speicherplätze für bestimmte Informationen zum Protokollablauf und/oder zur Datenzugriffskontrolle vorhanden sind.

30. Vorrichtung nach Anspruch 29, **dadurch gekennzeichnet,** daß im Zustandsspeicherbereich (ZS) zum Protokollablauf je ein Speicherplatz für die Blocknummer (STB) der der vorliegenden Anwendung zugeordneten Steuerliste (STL), ein Basisfunktionsspeicherplatz (BZ) für die Basisfunktionsbezeichnung (Bk) der zuletzt erfolgreich ausgeführten Basisfunktion (B) und ein Protokollzustandsspeicherplatz (Zi) für den Protokollzustand (Z) nach der zuletzt erfolgreich ausgeführten Basisfunktion (B) vorhanden ist.

31. Vorrichtung nach mindestens einem der vorhergehenden Ansprüche 29 oder 30, **dadurch gekennzeichnet,** daß die im Zustandsspeicherbereich (ZS) vorhandenen Speicherplätze zur Datenzugriffskontrolle in globale und in anwendungsbezogene Speicherplätze aufgeteilt sind.

32. Vorrichtung nach Anspruch 31, **dadurch gekennzeichnet,** daß je ein Speicherplatz für das anwendungsbezogene Speichern einer durchgeführten PIN-Prüfung (PIN) für einige sich voneinander unterscheidende durchgeführte Authentizitätsprüfungen (AUTH1,AUTH2) und ein globaler Speicherplatz für das Speichern einer durchgeführten PIN-Prüfung (GPIN) vorhanden sind.

FIG 1

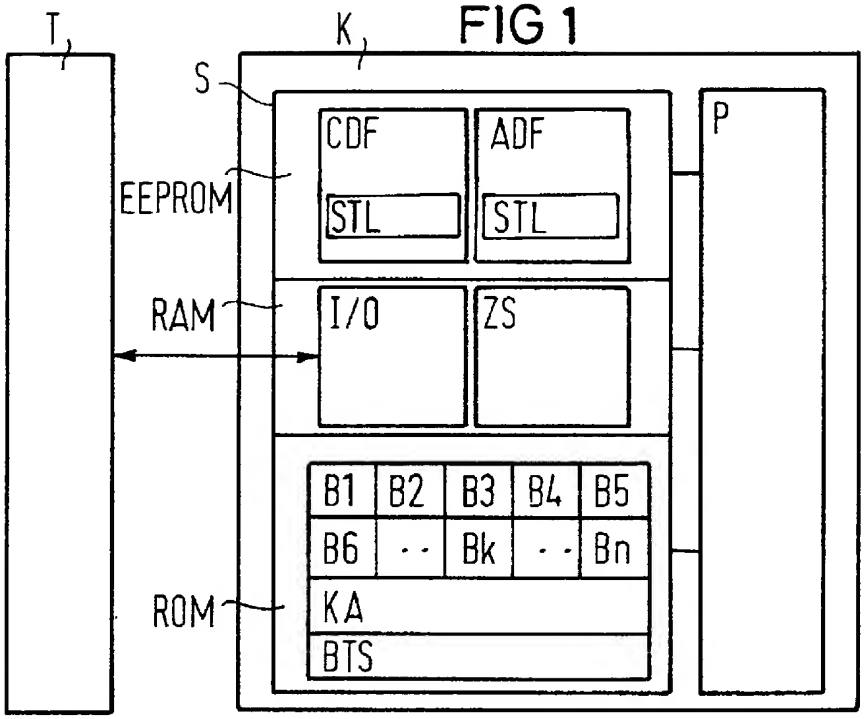

T
K
S
CDF
ADF
STL
STL
P
EEPROM
RAM
I/O
ZS
B1
B2
B3
B4
B5
B6
- -
Bk
- -
Bn
ROM
KA
BTS

FIG 2

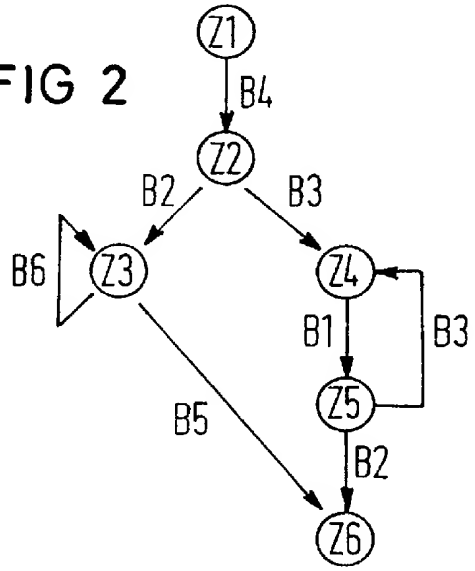

Z1
B4
Z2
B2
B3
B6
Z3
Z4
B1
B3
Z5
B5
B2
Z6

FIG 3

Z	BA	B	ZF	B	ZF	B	ZF
1	2	B4	Z2	B6	Z1	—	—
2	3	B2	Z3	B3	Z4	B6	Z2
3	2	B5	Z6	B6	Z3	—	—
4	2	B1	Z5	B6	Z4	—	—
5	3	B2	Z6	B3	Z4	B6	Z5
6	2	B6	Z6	—	—	—	—

FIG4

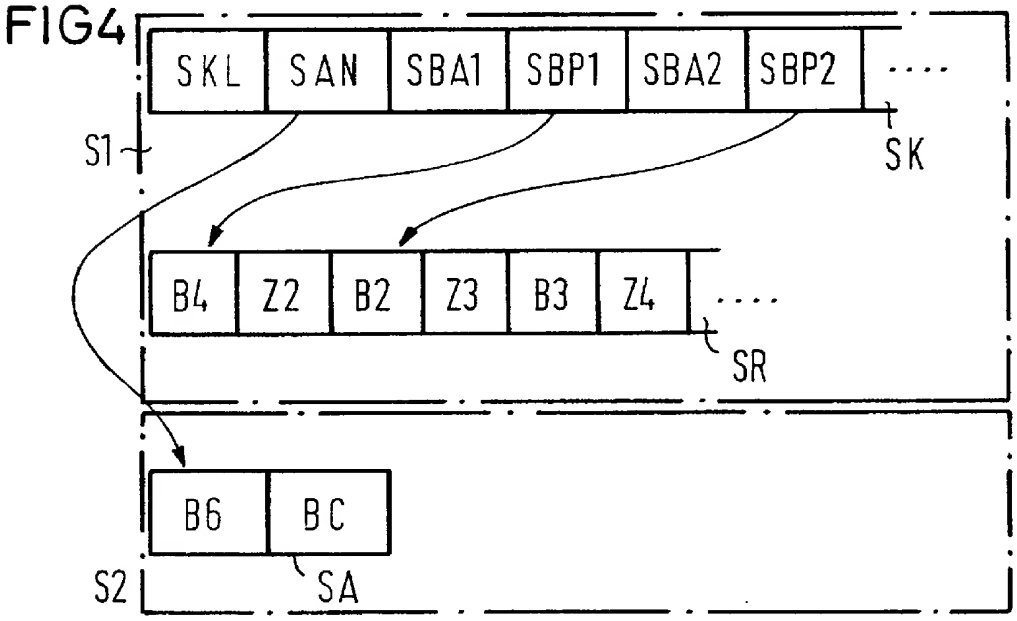
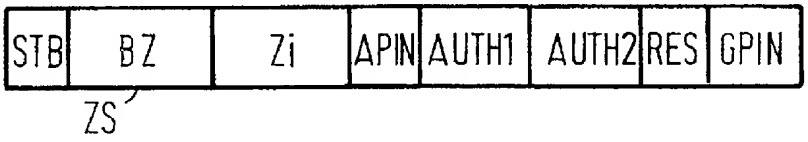


FIG 5



Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung

EP 90 11 3990

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int. Cl.5)
A	DE-A-3 736 190 (HITACHI) * Zusammenfassung; Ansprüche ; Figuren *	1-3, 10-13,20, 21,29-32	G 07 F 7/10
A	EP-A-0 190 733 (TOSHIBA) * Zusammenfassung; Figuren * * Seite 4, Zeile 23 - Seite 8, Zeile 13; Ansprüche *	1,21	
A	WO-A-8 707 062 (AMERICAN TELEPHONE AND TELEGRAPH) * Ansprüche ; Figuren 1-6, 8 *	1,21,32	
A	EP-A-0 159 651 (OMRON TATEISI ELECTRONICS) * Zusammenfassung; Ansprüche ; Figuren *	1,21	

RECHERCHIERTE SACHGEBIETE (Int. Cl.5)
G 07 F G 06 K

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
Den Haag	04 April 91	DAVID J.Y.H.

KATEGORIE DER GENANNTEN DOKUMENTE

- X: von besonderer Bedeutung allein betrachtet
- Y: von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
- A: technologischer Hintergrund
- O: nichtschriftliche Offenbarung
- P: Zwischenliteratur
- T: der Erfindung zugrunde liegende Theorien oder Grundsätze
- E: älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
- D: in der Anmeldung angeführtes Dokument
- L: aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument